

THE HONORABLE _____

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE**

STATE OF WASHINGTON,

Plaintiff,

v.

ADSCEND MEDIA, LLC, a Delaware
limited liability company; and JEREMY
BASH and FEHZAN ALI, individually
and as Managing Members of
ADSCEND MEDIA LLC,

Defendants.

NO.

COMPLAINT FOR INJUNCTIVE
AND ADDITIONAL RELIEF
UNDER THE CAN-SPAM ACT,
THE UNSOLICITED
COMMERCIAL EMAIL ACT,
AND THE CONSUMER
PROTECTION ACT

COMES NOW, Plaintiff, State of Washington ("the State"), by and through its attorneys Rob McKenna, Attorney General, and Paula Selis, Senior Counsel, and brings this action against Defendants named herein. The State alleges the following on information and belief:

I. INTRODUCTION

1.1 Adscend Media, LLC, ("Adscend"), Fehzan Ali and Jeremy Bash (collectively, "Defendants") pay their affiliates to deceive Facebook users and to initiate the sending of unsolicited commercial email messages ("spam") across Facebook's platform. As a result of

1 these actions, the State brings this action under the Controlling the Assault of Non-Solicited
 2 Pornography and Marketing Act ("CAN-SPAM Act"), 15 U.S.C. §§ 7701-7713. The State seeks
 3 a permanent injunction and other equitable relief, including damages and attorneys' fees, based on
 4 Defendants' violations of the CAN-SPAM Act.

5
 6 1.2 As part of the same case or controversy, the State also brings this action
 7 pursuant to RCW 19.190, the Commercial Electronic Mail Act ("CEMA"). The State seeks a
 8 permanent injunction and other equitable relief, including damages, civil penalties, and
 9 attorneys' costs and fees, based on violations of CEMA.

10 1.3 Finally, as part of the same case or controversy, the State also brings this action
 11 pursuant to RCW 19.86, the Consumer Protection Act. The State seeks a permanent injunction
 12 and other equitable relief, including damages, civil penalties, and attorneys' costs and fees,
 13 based on violations of the Consumer Protection Act.
 14

15 II. JURISDICTION AND VENUE

16 2.1 This Court has jurisdiction over this matter pursuant to 28 U.S.C. §§ 1331,
 17 1337(a), 28 U.S.C. § 1367 and 15 U.S.C. § 7706.

18 2.2 Venue in this district is proper under 28 U.S.C. § 1391 and 15 U.S.C. § 7706. A
 19 substantial portion of the acts complained of have occurred in King County and elsewhere in
 20 the Western District of Washington.
 21

22 III. PARTIES

23 3.1 The State, as *parens patriae*, is authorized by 15 U.S.C. § 7706(f) to file actions
 24 in federal district court to enjoin violations of the CAN-SPAM Act, to seek recovery for actual
 25 monetary loss or damages of up to \$250 per violation on behalf of Washington residents, and
 26

1 to obtain such further and other relief as the Court may deem appropriate, including treble
2 damages and attorneys' fees. The State is authorized by RCW 19.86.080 to enjoin violations
3 of the Consumer Protection Act, obtain restitution on behalf of persons harmed by such
4 violations, and obtain further and other relief as the Court may deem appropriate, including
5 civil penalties and attorneys' fees. The State is also authorized to file actions enjoining
6 violations of CEMA and to seek damages of \$500 per violation of its provisions pursuant to
7 RCW 19.190.040.
8

9 3.2 Defendant Adscend is a Delaware limited liability company. Adscend is
10 located at 1521 Concord Pike, Suite 202, Wilmington, Delaware 19803-3645. Adscend is an
11 advertising company that uses its proprietary network of affiliates to drive traffic to its
12 customers' websites. It transacts or has transacted business in the state of Washington and in
13 the Western District of Washington.
14

15 3.3 Defendant Jeremy Bash is a Managing Member and co-owner of Adscend and
16 as such, controls its policies, activities, and practices, including those alleged in this
17 Complaint. Defendant Bash resides at 3221 Bradley Road, Huntington, West Virginia 25704-
18 2725. Defendant Bash resides in the state of West Virginia and transacts or has transacted
19 business in the state of Washington and in the Western District of Washington.
20

21 3.4 Defendant Fehzan Ali is a Managing Member and co-owner of Adscend and as
22 such, controls its policies, activities, and practices, including those alleged in this Complaint.
23 Defendant Ali resides at 2707 Rio Grande Street, Suite 402, Austin, Texas 78705-4158.
24 Defendant Ali resides in the state of Texas and transacts or has transacted business in the state
25 of Washington and in the Western District of Washington.
26

IV. NATURE OR TRADE OF COMMERCE

A. How Facebook Works

4.1 Facebook is a “social utility”—a network that helps users communicate more efficiently and effectively with their friends, families and coworkers. To access Facebook’s computer network, information, features and services, a person must sign up, establish a unique username and password, and agree to the Facebook’s terms and conditions.

4.2 Once a user obtains a Facebook account, the user has access to his or her personal “profile,” which may be populated with information about the user. Facebook users may connect their profiles to the profiles of other users as Facebook “friends.” A Facebook friendship is mutual; both users must accept and agree to be friends before a connection is established.

4.3 Facebook users can also create “Pages,” which are similar to profiles but are generally used to promote businesses, charities or specific causes. According to Facebook’s policies, the administrator of the Page must be a Facebook user and an authorized representative of the subject of the Page.

4.4 Facebook users may connect their profiles to Facebook Pages by clicking on the “Like” button that is located on the top of each Page. If a Page is “liked,” a link to the Page is displayed on the user’s profile in a list under one of the categories such as “music,” “books,” or “interests” in the “Info” section of the user’s profile.

4.5 Once a Facebook user connects his or her profile to his or her friends’ profiles and other Pages, Facebook facilitates and enables connected profiles and Pages to communicate with each other. Facebook users may only be contacted through Facebook by

1 other registered Facebook users or by Facebook itself. Each user profile and each Facebook
2 Page has "Wall," which is an area where registered users with access to the profile or Page
3 may post content. Facebook Pages also have "Walls." Only registered users may post
4 messages on the Walls of other Facebook users. Recently, Facebook introduced "Timeline,"
5 which converts a profile to a "Timeline," and organizes all posts and content in the
6 chronological order that they are posted. Once a profile is converted to "Timeline," there is no
7 separate "Wall;" all content is simply posted to the Timeline. As of the filing of this
8 Complaint, not all profiles have converted to Timeline, and Facebook Pages continue to have
9 traditional "Walls" for posting content.
10

11 4.6 In addition to the user's profile, which contains the Wall or Timeline, Facebook
12 provides each user with a "News Feed" or "Home" Page. The News Feed displays, among
13 other things, activities performed by each of the user's friends, and Facebook Pages to which
14 the user has connected his or her profile. For example, a user's News Feed on a given day
15 could include updates posted by the user's friends, Pages to which the user has connected,
16 notices that friends became friends with other Facebook users, and notices that new content
17 was added to a friend's Wall or Timeline.
18

19 4.7 Whenever a Facebook user "Likes" a Facebook Page, a message announcing
20 that the user "Liked" the Page may be displayed in each of that user's friends' News Feeds.
21 The message may also contain a link to the Facebook Page that the user's friends can click to
22 visit the Page (and potentially decide whether to "Like" the Page themselves).
23
24
25
26

1 4.8 In addition to providing a platform for social networking, Facebook also
 2 provides users with tools that help them ensure that their accounts are not used by others, and
 3 the ability to adjust their personal privacy settings.

4 **B. Defendants' Unfair and Deceptive Business Activities**

5 4.9 Adscend, Bash and Ali (collectively, "Defendants") operate an affiliate
 6 advertising network that targets Facebook's networking platform with deceptive unsolicited
 7 messages couched as messages from users' friends. In fact, the messages are part of a scheme
 8 to market the services of Defendants' advertising clients. Defendants' advertising scheme is
 9 designed to trick Facebook users into allowing spam to be sent to all of their Facebook friends.
 10 While the subjects and contents of these messages vary from advertising campaign to
 11 campaign, all of them deceive Facebook users in two ways: (1) they do not identify the
 12 Defendants or their affiliates as the initiators and senders of the messages, and (2) they do not
 13 disclose that the messages are advertisements, despite the fact that the messages' sole purpose
 14 is to lure users to participate in deceptive advertising scams if they click on the links presented
 15 in the posts. Given Facebook's social environment, users unwittingly click on the links
 16 because they believe the links were sent by their own Facebook friends.

17 4.10 As described on Defendants' website, <http://adscendmedia.com>, Adscend is an
 18 advertising company that operates an affiliate marketing program, otherwise known as a Cost
 19 Per Action, or "CPA," marketing program. Under this program, Defendants recruit
 20 individuals, or "affiliates," to create advertisements that drive traffic to Internet websites that
 21 have contracted with Defendants. Under the CPA marketing model, the contracting website, or
 22 "advertiser," pays Defendants, who in turn pay their affiliates, for the traffic that Defendants'
 23
 24
 25
 26

1 affiliates generate only when some specific action is taken by the user on the website, such as
2 participating in a promotional survey sponsored by the advertiser, completing an offer for a gift
3 card, or making a purchase of some sort.

4 4.11 Defendants create and provide their affiliates with technology that is designed
5 to deceive Facebook users into visiting websites that pay Defendants for the referral traffic.
6 This technology, called a "content locking widget," is a software script that places a box over
7 and in front of the content on a website. Unless and until the visitor to the website completes
8 certain actions within the widget, the box will remain and cover the content of the website—
9 thereby "locking" the desired content from the visitor's view.
10

11 4.12 Defendants encourage and pay their affiliates to create Facebook Pages that are
12 titled and designed to "bait" users into visiting other websites. These bait pages appear in
13 posts that seemingly originate from Facebook users' friends. The bait pages offer visitors an
14 opportunity to view enticing or salacious content, such as "[Video] OMG! See What Happens
15 to his Ex Girlfriend" that displays what appears to be an embedded online video with a picture
16 of a scantily-clad woman hidden behind the content locking widget, or "Cannot BELIEVE a 2
17 year old is doing THIS," with text that states "You will be SHOCKED when you see the video.
18 Simply "Like" this page to see the video."
19

20 4.13 The following screenshot progression is an example of a typical Adscend
21 promotion. It begins with the appearance of a post on a user's News Feed page that seemingly
22 comes from the user's friend. It entices the user by providing a salacious picture next to a link
23 to a Bait Page that promises "[Video] OMG! See what happened to his Ex Girlfriend!":
24
25
26

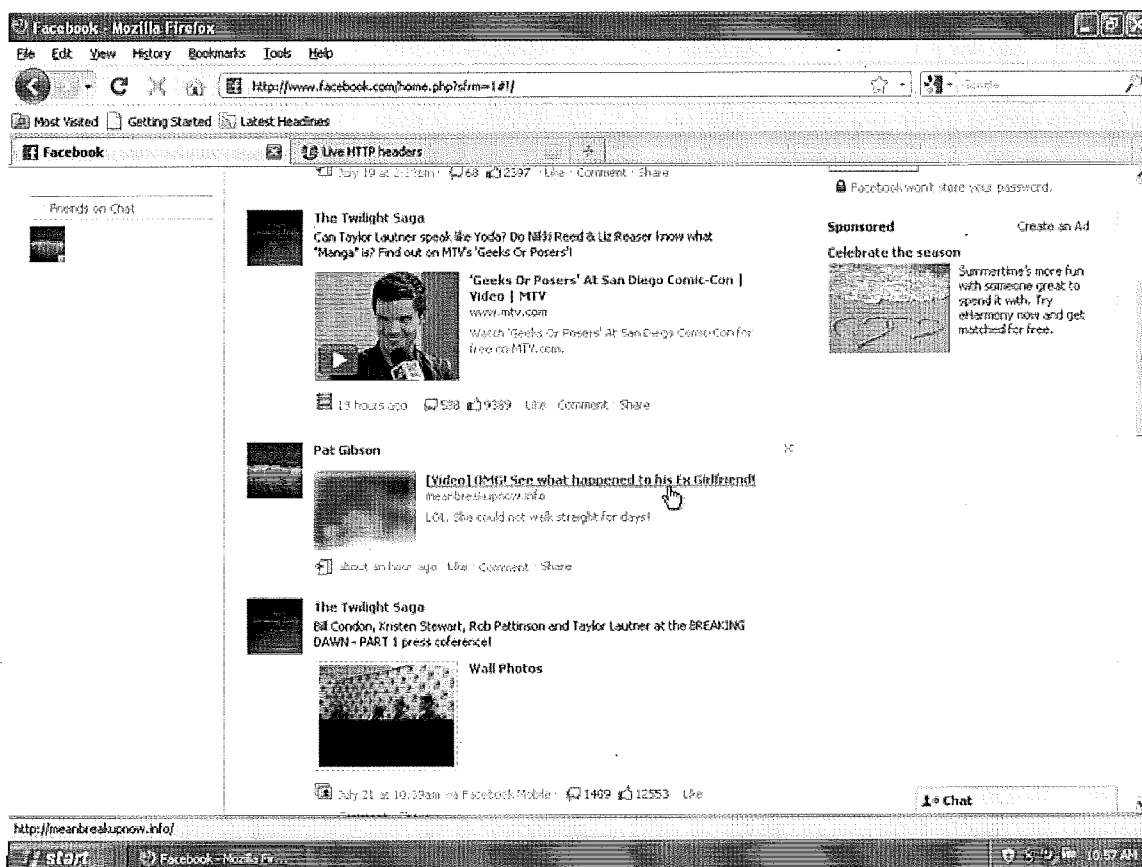


Figure 1

4.14 If the user clicks on the link, he or she is navigated to the Bait Page that is designed to look like the promised content is available on it. The following is the Bait Page to which the user is taken when he or she clicks on the post that advertises “[Video] OMG! See what happened to his Ex Girlfriend!”:

///



Figure 2

4.15 But before the user can supposedly access the content, Defendants navigate him or her to a second Bait Page and interpose a "content-locking widget," a small window placed in front of the promised content to block the visitor from actually viewing it. On this second Bait Page, shown in Figure 3, the user is confronted with the content-locking widget, disguised as an "Age Verification" notice which blocks the user's access to the video. The widget is intended to mislead the users into thinking that Facebook's security policies require the user to verify his or her age before the content can be viewed. However, the "Age Verification" check is not associated with Facebook in any way.



Figure 3

4.16 When the user clicks on the button to verify his or her “age,” he or she unknowingly activates the “Share” function of Facebook, which causes the advertisement for the Bait Page to appear in the Facebook News Feeds of all of the users’ Facebook friends. The user’s browser is then redirected to another Page that appears to be the beginning of the salacious video content. In fact, it is a Page that allows Adscend to track the user’s activity. See Figure 4.



Figure 4

4.17 Then, without the user taking any additional action, yet another content-locking widget appears as an overlay on this landing page, with the “Age Verification” heading again. This “Age Verification” widget requires even more from the user as a condition to viewing the promised content. As demonstrated in Figure 5 below, the user must take one of six surveys, with a promise that it will take only 20 seconds to complete:

///

///

///

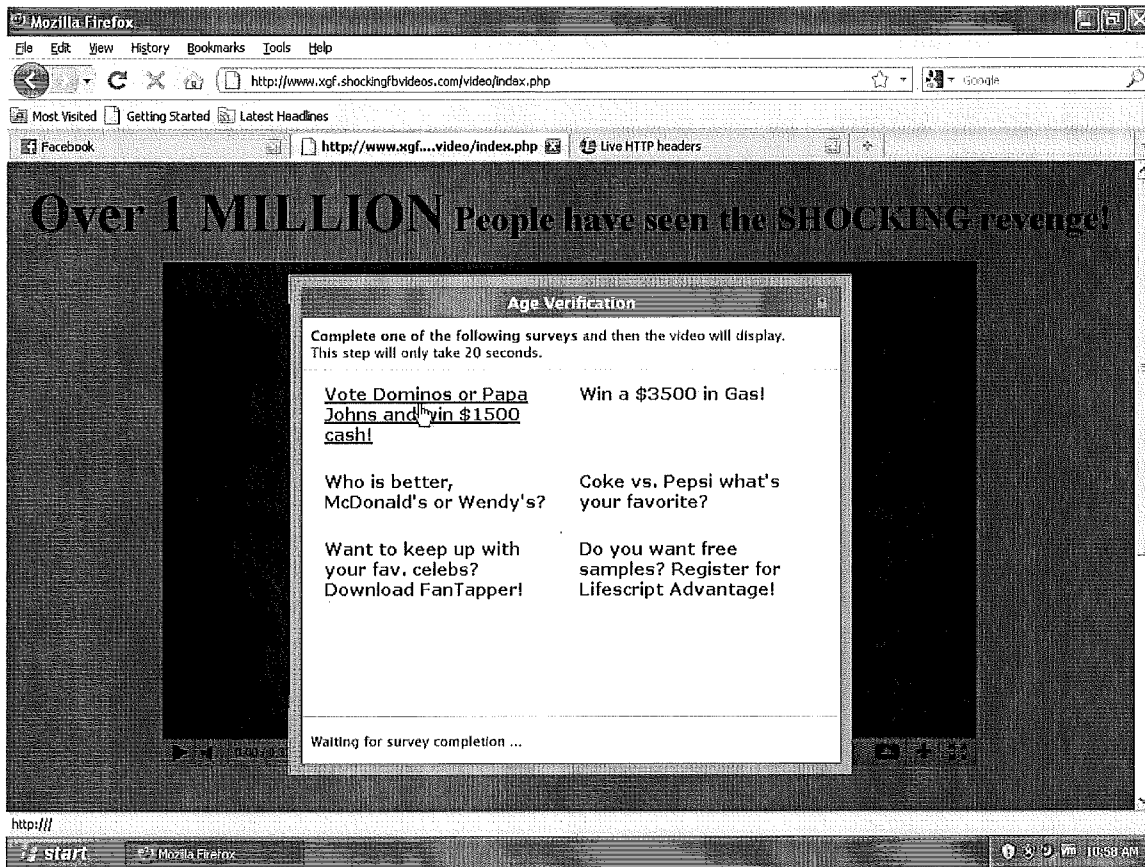


Figure 5

4.18 The hyperlinks to the surveys actually lead to other landing Pages that contain information fields that take far more than 20 seconds to complete. The “surveys” included in Figure 5 are actually a group of links to special advertising websites that provide revenue to Defendants. If the user clicks on one of the links and, for example, provides personal information to one of Defendants’ advertisers, Defendants are paid a commission. The “survey” is actually a device designed and provided by Defendants to extract personal information from the user or require the user to purchase goods and services. See Figure 6, a typical example of a “survey” form.

///

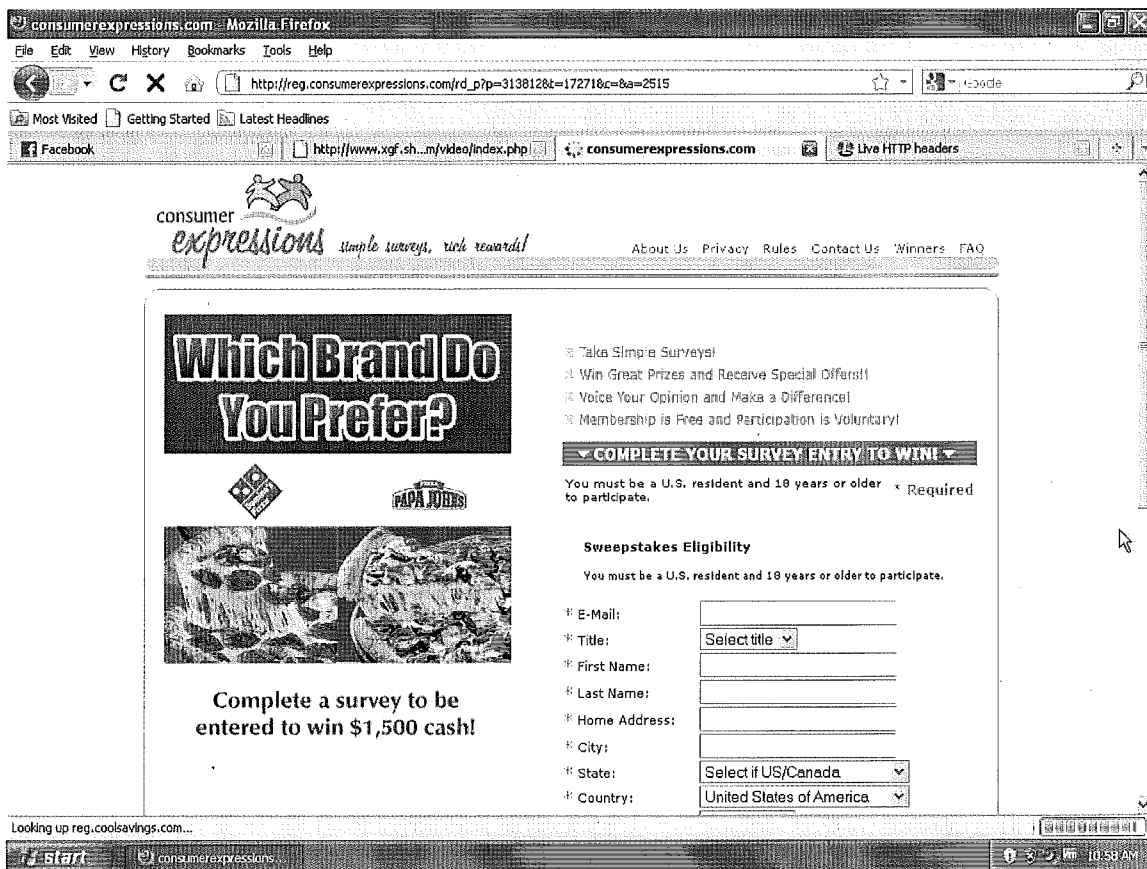


Figure 6

4.19 While the user is viewing the surveys and promotional information, Adscend is tracking which of its affiliates successfully lured the particular user to visit the advertiser's survey or other promotion. The information is tracked by the affiliate's unique identifier ("Affiliate ID").

4.20 Despite the fact that the entire purpose of Defendants' advertising scheme is to promote its advertisers' good and services, the initial posts that ensnare the users into Defendants' scheme make no reference to the goods or services ultimately promoted on the CPA advertising sites. Although the posts that lure users to Bait Pages have varied, they have been consistently designed to entice the user into clicking on them. For example, the posts

1 have stated “(My) mom took my computer away when she found out I Googled this,” and
 2 “(T)his man took a picture of his face every day for 8 years!!”

3 4.21 Though the opening ploy of Defendants’ scheme may differ, the goal is always
 4 the same—to trick the user into navigating to the Bait Page containing the locked content and
 5 the surveys. And in many instances, the promised content is not even delivered. It is an empty
 6 promise used to bait Facebook users into Defendants’ marketing scheme.
 7

8 4.22 In addition to misleading users with deceptive posts and Bait Pages,
 9 Defendants’ advertising scheme is designed to propagate itself virally throughout the Facebook
 10 system. Before the user is directed to the Bait Page, he or she sometimes asked to “Like” or
 11 “Share” the page, or is directed to an intermediary Page that in some instances instructs the
 12 user to simply “Click Here.” Figure 7 is one example of one of the intermediary Pages:
 13



14
 15 Click here to continue
 16
 17
 18
 19

20 Figure 7

21 4.23 Hidden behind the “Click here to continue” link in Figures 7 is source code for
 22 the “Like” feature of Facebook. When a user clicks on “Click here to continue,” it activates the
 23 “Like” responses within Facebook, and the advertisement for the Bait Page is posted to the
 24 user’s Wall or Timeline and published in the Facebook News Feeds of all of the users’
 25 Facebook friends. Figure 3 in Paragraph 4.16 also contains a similar button—the “Share”
 26

1 button, which has a functionality similar to the "Like" button, insofar as clicking on it spreads
2 the advertisement to friends' News Feeds. By using these methods, Defendants are able to
3 hijack Facebook users' accounts in order to cause them to virally propagate spam messages
4 advertising the "Liked" or "Shared" Page to other Facebook users. Hijacking a Facebook user's
5 account and "Liking" Facebook Pages on the user's behalf without his or her knowledge is
6 known within the affiliate marketing community as "Likejacking."

8 4.24 Defendants' advertising customers pay them whenever a user interacts with the
9 survey widget and either surrenders the requisite personal information or purchases the
10 products advertised within the widget. Then, Defendants in turn pay a commission from that
11 payment to the affiliates for getting the visitors to interact with the widget. Defendants provide
12 the platform and technology for their affiliates to utilize the content-locking widget. They also
13 provide the platform and technology necessary to track the traffic referred by their affiliate
14 marketers. When an affiliate succeeds in getting a Facebook user to access the widget,
15 Defendants' tracking technology records the Affiliate ID for that affiliate and tracks the actions
16 of the person using the widget. Tracking Internet traffic to and through Defendants' widget by
17 Affiliate ID allows Defendants to determine the proper commission to pay each affiliate.
18

19 4.25 The vast majority of Defendants' revenue is obtained through Facebook
20 advertising. At the inception of Defendants' business, approximately 80% of their income was
21 derived from Facebook solicitations. Their income has included gross monthly revenues of up
22 to \$1.2 million. As an example of Defendants' ability to obtain advertising traffic, in February
23 2011, their affiliates tricked 280,214 Facebook users into visiting their "locked content" pages
24 through spam solicitations.
25
26

1 4.26 Defendants are aware that most of their business is obtained through Facebook
 2 solicitations and that their affiliates have used spam to distribute links to Facebook users. In
 3 some instances, they actually have reviewed and approved the advertising campaigns of their
 4 affiliates before the campaigns were run on Facebook. They assiduously track the user traffic
 5 that leads to their advertisers' offers. They know that the Facebook social network is the
 6 largest single source of their advertising revenue. Defendants know that their affiliates use the
 7 devices described above to attract users to the "locked content," and that Facebook has been
 8 the most effective way for them to sell their advertisers' services. Defendants compensate
 9 their affiliates, intentionally paying them to send commercial solicitations through Facebook.
 10 Even though Defendants know their affiliates use spam to distribute links to Facebook users,
 11 they continue to permit the deceptive spam. Defendants consciously have continued to support
 12 and pay for the traffic from these campaigns because of the substantial amount of revenue the
 13 campaigns generate.
 14
 15

16 4.27 Defendants are in competition with others in the State of Washington engaged
 17 in online advertising .
 18

19 **V. VIOLATIONS OF THE CAN-SPAM ACT**

20 5.1 Plaintiff realleges paragraphs 4.1 through 4.28 and incorporates them herein as
 21 if set forth in full.

22 5.2 The CAN-SPAM Act makes it unlawful to initiate the transmission of an email
 23 that contains materially misleading or materially false header information. 15 U.S.C.
 24 § 7704(a)(1). The term "materially" includes the alteration or concealment of header
 25 information that would impair the ability of a law enforcement agency, among other entities, to
 26

1 identify the initiator of the email message or to investigate an alleged violation of the Act.
2 15 U.S.C. § 7704(a)(6). The Act also makes it unlawful to initiate email with misleading
3 subject lines. 15 U.S.C. § 7704(a)(2). The Act requires commercial electronic mail to contain
4 conspicuous notice that the message is an advertisement. 15 U.S.C. § 7704(a)(5)(A)(i),(ii).
5 The term “initiate” means “to originate or transmit” or “to procure the origination or
6 transmission of” a commercial electronic message. 15 U.S.C. § 7702(9). The term “procure”
7 means to intentionally pay or provide other consideration to another to initiate a commercial
8 electronic message. 15 U.S.C. § 7702(12).
9

10 5.3 The primary purpose of the electronic messages Defendants’ affiliates send
11 through the Facebook site, including but not limited messages to Wall posts, News Feeds, and
12 Page suggestions, is the commercial advertisement or promotion of a product or service. All of
13 these messages are “commercial electronic mail messages” as defined by 15 U.S.C § 7702(2)(A).
14

15 5.4 Defendants intentionally pay their affiliates to send commercial electronic mail
16 messages through the Facebook site, and thereby “procure” the origination of such messages, as
17 that term is defined in 15 U.S.C § 7702(12). By “procuring” the origination of such messages,
18 Defendants thereby “initiate” commercial electronic mail messages, as that term is defined by
19 15 U.S.C § 7702(9). Defendants procure the sending of electronic mail messages through their
20 affiliates on the Facebook site, knowing that those commercial electronic mail messages violate
21 the provisions of the CAN SPAM Act.
22

23 5.5 In violation of 15 U. S.C. § 7704(a)(1), Defendants, through their affiliates,
24 mislead Facebook users by initiating commercial electronic mail messages that contain header
25 information that is materially false or misleading as to the true identity of the initiator of the
26

1 messages. The messages appear to originate from the user's friends, whose names appear in
2 proximity to the messages themselves, when in fact they are sent through an automatically-
3 generated mechanism specifically designed to mislead the user as to the message's source.

4 5.6 In violation of 15 U.S.C § 7704(a)(2), Defendants, through their affiliates,
5 initiate commercial electronic mail messages that mislead Facebook users about a material fact
6 regarding the contents or subject matter of the message. Defendants know or should know, on
7 the basis objective circumstances, that Facebook users are misled into clicking on messages
8 with the reasonable expectation that the message comes from one of their friends. The
9 messages lure users by promising views of salacious, strange or shocking contents, but fail to
10 disclose that they are actually the gateway to advertisements for Defendants' advertisers'
11 services. They further fail to disclose that in order to view the promised content, the user must
12 first "unlock" it by providing information, taking a survey, subscribing to a service, or
13 performing some other action consistent with Defendants' advertisers' requirements.
14 Additionally, in many instances, the "locked content" does not even deliver what is promised.
15 In some instances, the content is not "unlocked" even when the user participates in an offer,
16 and there is nothing available to view.

17 5.7 Additionally, in violation of 15 U.S.C. § 7704(a)(5), Defendants, through their
18 affiliates, initiate commercial electronic mail messages that do not contain clear and
19 conspicuous identification that the messages are advertisements or solicitations. The messages
20 appear to be personal communications sent from users' friends, rather than commercial
21 solicitations designed to market products and services.
22
23
24
25
26

5.8 The State has reason to believe that Defendants' conduct as described above has adversely affected Washington residents by violating 15 U.S.C §§ 7704(a)(1)(2) and (5), and pursuant to 15 U.S.C. § 7706(f)(1), seeks to enjoin further violations of Section 7704 and to obtain money damages on behalf of the residents of the State in an amount to be proven at trial pursuant to 15 U.S.C. § 7706(f)(3).

5.9 Plaintiff seeks an award of aggravated damages pursuant to 15 U.S.C. § 7706(f)(3)(C), in an amount to equal three times the amount otherwise available on the basis that Defendants committed the violations described herein willfully and knowingly.

5.10 Plaintiff seeks an award of the costs of this action and reasonable attorney fees, pursuant to 15 U.S.C. § 7706(f)(4).

VI. VIOLATIONS OF WASHINGTON'S COMMERCIAL ELECTRONIC MAIL ACT

6.1 Plaintiff realleges Paragraphs 4.1 through 5.10 and incorporates them herein as if set forth in full.

6.2 CEMA prohibits misrepresenting or obscuring any information in identifying the point of origin or the transmission path of a commercial electronic mail message. RCW 19.190.020(1)(a). It also prohibits the transmission of commercial electronic mail messages that contain false or misleading information in the subject line. RCW 19.190.030(1)(b). The Act applies to not only those who initiate the transmission of commercial electronic mail messages, but also to those who “assist the transmission” by providing “substantial assistance or support” to those who initiate the messages. RCW 19.190.010(1).

6.3 The primary purpose of the electronic messages sent by Defendants' affiliates through the Facebook site, including but not limited to Wall posts, News Feeds, and Page

1 suggestions, is to promote goods or services for sale. The messages are “commercial electronic
2 mail messages” as defined in RCW 19.190.010(2).

3 6.4 Defendants assist the transmission of their affiliates’ commercial electronic mail
4 messages on the Facebook site by compensating them each time a user clicks on a link, purchases
5 or subscribes to an advertiser’s services, or takes some other type of prescribed action.
6 Defendants also assist in the transmission of the messages by providing a platform that enables
7 their affiliates to operate. They walk their affiliates through a “short setup process,” in which they
8 send them a line of HTML code to place on the affiliates’ web page. This enables the affiliate to
9 display the “gateway” over the web page itself (i.e. the “content-locking widget” that prevents the
10 user from viewing the page until he or she completes a survey or take some other type of action).
11 See Figure 5 above.
12

13 6.5 Additionally, Defendants provide the promotional offer language contained in the
14 widget itself and the template for the widget background. Finally, they provide the platform and
15 technology necessary to track traffic referred by their affiliate marketers, and directly compensate
16 them based on this tracking system. It is only with Defendants’ substantial assistance and support
17 that their affiliates are able to market through commercial electronic mail messages on Facebook.
18 Accordingly, Defendants “assist the transmission” of commercial electronic mail messages as that
19 term is defined in RCW 19.190.010(1). Defendants provide this substantial assistance and
20 support, knowing or consciously avoiding knowing, that their affiliates are engaged, or intend to
21 engage, in practices that violate the Consumer Protection Act, RCW 19.86. A violation of
22 CEMA is a violation of the Consumer Protection Act. RCW 19.190.100.
23
24
25
26

1 6.6 Defendants, through their affiliates, assist in the transmission of commercial
 2 electronic mail messages on the Facebook site that misrepresent information in identifying the
 3 messages' point of origin in violation of RCW 19.190.020(1)(a). The messages appear to
 4 originate from the user's friends, whose names appear in proximity to the messages themselves,
 5 when in fact they are sent through an automatically-generated mechanism specifically designed to
 6 mislead the user as to the message's source. The messages are sent to electronic mail addresses
 7 that the sender knows or has reason to know are held by Washington residents.
 8

9 6.7 Defendants' conduct as described in Paragraph 6.6 above also violates the
 10 Consumer Protection Act, pursuant to RCW 19.190.030(2) which states that it is a violation of the
 11 Consumer Protection Act to assist in the transmission of commercial electronic mail messages
 12 that misrepresent information in identifying the messages' point of origin. Defendants provide
 13 this assistance, knowing or consciously avoiding knowing that their affiliates are engaged, or
 14 intend to engage in conduct that violates RCW 19.190.020(a) and the Consumer Protection Act.
 15

16 6.8 Defendants, through their affiliates, assist in the transmission of commercial
 17 electronic mail messages on the Facebook site that contain false or misleading information in the
 18 subject line in violation of RCW 19.190.020(1)(b). The messages lure users by promising views
 19 of salacious, strange or shocking contents, but fail to disclose that in order to do so, the user must
 20 first visit the "locked content" site. For example, the message may claim to link to a video of
 21 "[Video] OMG! See what happened to his Ex Girlfriend!" or "This man took a picture of his face
 22 every day for 8 years!!" The messages fail to disclose that they are actually the gateway to
 23 advertisements for Defendants' advertisers' services. They further fail to disclose that in order to
 24 view the promised content, the user must first "unlock" it by providing information, taking a
 25
 26

1 survey, subscribing to a service, or performing some other action consistent with Defendants'
 2 advertisers' requirements. Additionally, in many instances, the "locked content" does not even
 3 deliver what is promised. The messages are sent to electronic mail addresses that the sender
 4 knows or has reason to know are held by Washington residents.

5
 6 6.9 Pursuant to RCW 19.190.030(2), Defendants' conduct as described in
 7 Paragraph 6.8 also violates the Consumer Protection Act, because Defendants assist in the
 8 transmission of commercial electronic mail messages that contain false or misleading information
 9 in the subject line. Defendants provide this assistance, knowing or consciously avoiding knowing
 10 that their affiliates are engaged, or intend to engage in conduct that violates
 11 RCW 19.190.020(1)(b) and the Consumer Protection Act.

12
 13 6.10 As authorized by RCW 19.86.080 the State seeks to enjoin Defendants from
 14 further violations of CEMA and the Consumer Protection Act. The State also seeks to recover
 15 damages of \$500 per violation of CEMA. RCW 19.190.040(1). Pursuant to RCW 19.86.140,
 16 Plaintiff further seeks an award of civil penalties for each of Defendants' violations of the
 17 Consumer Protection Act, in an amount of up to \$2,000 per violation. Plaintiff also seeks recover
 18 its costs, including reasonable attorneys' fees, pursuant to RCW 19.86.080.

19 **VII. VIOLATIONS OF WASHINGTON'S CONSUMER PROTECTION ACT**

20
 21 7.1 Plaintiff realleges paragraphs 4.1 through 6.10 and incorporates them herein as if
 22 set forth in full.

23 7.2 Defendants provide a platform that enables their affiliates to operate in a deceptive
 24 manner. Defendants set up their affiliates with the necessary HTML code that enables the
 25 affiliates to display the "gateway" dialogue box over the affiliate web page itself (i.e. the "content-
 26

locking widget”). In addition to the “lock” for the content, Defendants provide an array of templates for affiliates to use as the part of the gateway dialogue box. Defendants design some of these templates to appear as though they originate directly from Facebook. The following is an example of the content-locking widget Defendants provide to their affiliates:

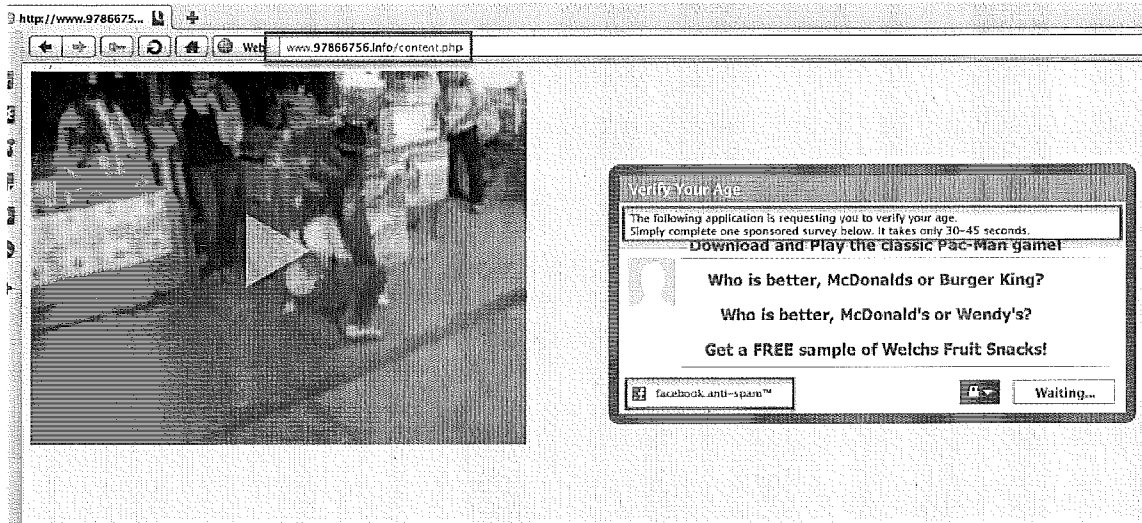


Figure 8

7.3 In this example, Defendants’ template, provided to and used by its affiliates, displays the Facebook logo; contains the heading “verify your age;” is specifically (and falsely) labeled “Facebook anti-spam;” and appears to be a security measure taken by Facebook itself to protect its own network. The colors and typeface used in the dialogue box are those used by Facebook in its official messages to its users, i.e. white on a blue background.

7.4 Defendants’ template simulates a Facebook dialogue box with the Facebook logo and a seemingly official Facebook message. In fact, the dialogue boxes are one step in a sequential advertising promotion. In this manner, Defendants misrepresent that their commercial solicitation is an actual message originating from Facebook itself, regarding age verification and Facebook’s anti-spam measures. Since both age verification and anti-spam measures are matters

1 about which Facebook has real concerns, Defendants are able to wrap what is otherwise a strictly
2 commercial solicitation in an official-seeming cloak of legitimacy that heightens the chances that
3 the user will click on the link.

4 7.5 Additionally, the statement that the user must “verify (his or her) age”
5 misrepresents not only the origin of the message, but its urgency. The user is seemingly told that
6 Facebook requires the user to take certain steps, pursuant to its own internal policies, in order to
7 continue viewing certain pages. By posting this seemingly urgent message, Defendants heighten
8 the chances that the user will click on the link. In fact, the user does not need to “verify (his or
9 her) age” in order to continue viewing the pages in the advertising progression.

10 7.6 In other examples of their promotions, Defendants represent that the user is
11 required to take a “security test to ensure the people on this site are real.” Users are further told
12 that they must complete a “free” survey” in order to “verify that (they) are human.” In fact, the
13 purpose of the survey is neither to perform a “security test” or ensure the user is “human.”
14 Rather, the purpose is to trick consumers into clicking on links to special CPA advertising sites
15 that provide revenue to Defendants. If the user clicks on one of the links and, for example,
16 obtains a gift card from one of Defendants’ advertisers, Defendants are paid a commission. The
17 “survey” is, in fact, a method designed to extract personal information from the user or require the
18 user to purchase goods and services.

19 7.7 Defendants’ misrepresentations, including but not limited to their use of the
20 Facebook logo; their use of the heading “verify your age;” their label “Facebook anti-spam”; their
21 use of Facebook’s colors and typeface; and their deceptive reasons for which the user is required
22 to take a “survey” or perform other actions in order to view locked content, are misrepresentations
23
24
25
26

1 that constitute unfair and deceptive acts or practices in trade or commerce and unfair methods of
 2 competition in violation of the Consumer Protection Act, RCW 19.86.020. Defendants' failure to
 3 disclose that their templates are, in fact, commercial solicitations, is material. Defendants' failure
 4 to disclose these material facts constitutes unfair and deceptive acts or practices in trade or
 5 commerce and unfair methods of competition in violation of the Consumer Protection Act,
 6 RCW 19.86.020.
 7

8 **VIII. THIS COURT'S POWER TO GRANT RELIEF**

9 8.1 The CAN-SPAM Act empowers this Court to enjoin further violations by
 10 defendants. 15 U.S.C. § 7706(f)(1)(A). This Court is also empowered to award the greater of
 11 actual or statutory damages. 15 U.S.C. § 7706(f)(1)(B).
 12

13 8.2 The Commercial Electronic Mail Act, RCW 19.190, may be enforced by this
 14 Court through pendant jurisdiction. 28 U.S.C. § 1367. This Court is empowered to award the
 15 greater of actual or statutory damages under the Act. RCW 19.190.040(1).
 16

17 8.3 The Consumer Protection Act, RCW 19.86, may be enforced by this Court
 18 through pendant jurisdiction. 28 U.S.C. § 1367. This Court is empowered to grant injunctive and
 19 such other relief as it may deem appropriate to halt and redress violations of the Consumer
 20 Protection Act, including civil penalties and costs and fees. RCW 19.86.080, 19.86.140.
 21

22 **IX. PRAYER FOR RELIEF**

23 WHEREFORE, Plaintiff, STATE OF WASHINGTON, prays that this Court grant the
 24 following relief:
 25

- 26 a. Adjudge and decree that Defendants have engaged in the conduct
 complained of herein;

- 1 b. Adjudge and decree that the conduct complained of in Paragraphs 5.1
2 through 5.7 constitutes violations of the CAN-SPAM Act, 15 U.S.C. §§
3 7701-7713;
4
5 c. Adjudge and decree that the conduct complained of in Paragraphs 6.1
6 through 6.8 constitutes violations of the Commercial Electronic Mail
7 Act, RCW 19.190, and pursuant to RCW 19.190.030(3), constitutes per
8 se violations of the Consumer Protection Act, RCW 19.86.
9
10 d. Adjudge and decree that the conduct complained of in paragraphs 6.1
11 through 6.8 and 7.1 through 7.7, constitutes unfair or deceptive acts or
12 practices in violation of the Consumer Protection Act, RCW 19.86;
13
14 e. Permanently enjoin Defendants and their representatives, successors,
15 assigns, officers, agents, servants, employees, and all other persons
16 acting or claiming to act for, on behalf of, or in active concert or
17 participation with Defendants from continuing or engaging in the
18 unlawful conduct complained of herein;
19
20 f. Award such relief as the Court finds necessary to redress injury to
21 consumers resulting from Defendants' violations of the CAN-SPAM
22 Act, the Commercial Electronic Mail Act, and the Consumer Protection
23 Act;
24
25 g. Assess a civil penalty, pursuant to RCW 19.86.140, of up to \$2,000 for
26 each violation of RCW 19.86.020 caused by the conduct herein;

1 h. Award Plaintiff the costs of bringing this action, pursuant to 15 U.S.C. §
2 7706(f)(4), RCW 19.86.080, as well as such other and additional relief
3 as the Court may determine to be just and proper.
4

5 DATED this 26th day of January, 2012.
6

7 Presented by:
8 ROBERT M. MCKENNA
9 Attorney General

10 By: /s/ Paula Selis
11 PAULA SELIS, WSBA 12823
12 Assistant Attorney General
13 Attorney General of Washington
14 800 5th Ave, Suite 2000
15 Seattle, WA 98104-3188
16 Phone: (206) 389-2514
17 Fax: (206) 587-5636
18 E-mail: Paula.Selis@atg.wa.gov
19 *Attorney for Plaintiff State of Washington*
20
21
22
23
24
25
26